Residual modular Galois representations: images and applications

Samuele Anni

University of Warwick

London Number Theory Seminar
King's College London, 20th May 2015

THE UNIVERSITY OF WARWICK

Let n be a positive integer. The **congruence subgroup** $\Gamma_1(n)$ of $\mathrm{SL}_2(\mathbb{Z})$ is the subgroup given by

$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : n \mid a-1 \,,\ n \mid c \right\}.$$

$\Gamma_1(n)$ acts on the complex upper half plane via fractional transformations.

Definition

We define the **modular curve** $Y_1(n)_{\mathbb{C}}$ to be the non-compact Riemann surface obtained giving on $\Gamma_1(n)\backslash\mathbb{H}$ the complex structure induced by the quotient map. Let $X_1(n)_{\mathbb{C}}$ be the compactification of $Y_1(n)_{\mathbb{C}}$.

The modular curve $Y_1(n)_{\mathbb{C}}$ can be defined algebraically over $\mathbb{Z}[1/n]$.

Let $n \geq 5$ and k be positive integers and let ℓ be a prime not dividing n. Following Katz, we define the space of **mod ℓ cusp forms** as

mod ℓ cusp forms

$$S(n,k)_{\overline{\mathbb{F}}_\ell} = \mathrm{H}^0(X_1(n)_{\overline{\mathbb{F}}_\ell}, \omega^{\otimes k}(-\mathrm{Cusps})).$$

$S(n,k)_{\overline{\mathbb{F}}_\ell}$ is a finite dimensional $\overline{\mathbb{F}}_\ell$-vector space, equipped with Hecke operators T_n $(n \geq 1)$ and diamond operators $\langle d \rangle$ for every $d \in (\mathbb{Z}/n\mathbb{Z})^*$.

The $\mathbb{Z}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(S(\Gamma_1(n),k)_{\mathbb{C}})$ generated by T_p and diamond operators $\langle d \rangle$ is the **Hecke algebra** $\mathbb{T}(n,k)$.

Analogous definition in characteristic zero and over any ring where n is invertible.

One may think that mod ℓ modular forms come from reduction of characteristic zero modular forms mod ℓ:

$$S(n,k)_{\mathbb{Z}[1/n]} \to S(n,k)_{\mathbb{F}_\ell}.$$

Unfortunately, this map is **not surjective** for $k = 1$.

Even worse: let $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a character, whose image is contained in $\mathcal{O}_K$, ring of integers of the number field K, then the map

$$S(n,k,\epsilon)_{\mathcal{O}_K} \to S(n,k,\overline{\epsilon})_{\mathbb{F}}$$

is **not** always **surjective** even if $k > 1$, where $\mathbb{F}$ is the residue field at ℓ and $\overline{\epsilon}$ is the reduction of ϵ.

$$S(n,k,\epsilon)_{\mathcal{O}_K} := \{f \in S(n,k)_{\mathcal{O}_K} \,|\, \forall d \in (\mathbb{Z}/n\mathbb{Z})^*, \langle d\rangle f = \epsilon(d) f\}.$$

$\mathbb{T}_\epsilon(n,k)$ will denote the associated Hecke algebra.

Theorem (Deligne, Serre, Shimura)

Let n and k be positive integers. Let $\mathbb{F}$ be a finite field of characteristic ℓ, with ℓ not dividing n, and $f : \mathbb{T}(n,k) \twoheadrightarrow \mathbb{F}$ a surjective morphism of rings. Then there is a continuous semi-simple representation:

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}),$$

unramified outside $n\ell$, such that for all p not dividing $n\ell$ we have:

$$\mathrm{Trace}(\rho_f(\mathrm{Frob}_p)) = f(T_p) \text{ and } \det(\rho_f(\mathrm{Frob}_p)) = f(\langle p \rangle)p^{k-1} \text{ in } \mathbb{F}.$$

Such a ρ_f is unique up to isomorphism.

Computing ρ_f is "difficult", but theoretically it **can be done in polynomial time** in $n, k, \#\mathbb{F}$:

Edixhoven, Couveignes, de Jong, Merkl, Bruin, Bosman ($\#\mathbb{F} \leq 32$):

Example: for $n = 1$, $k = 22$ and $\ell = 23$, the number field corresponding to $\mathbb{P}\rho_f$ (Galois group isomorphic to $\mathrm{PGL}_2(\mathbb{F}_{23})$) is given by:

$$\begin{aligned} & x^{24} - 2x^{23} + 115x^{22} + 23x^{21} + 1909x^{20} + 22218x^{19} + 9223x^{18} + 121141x^{17} \\ & + 1837654x^{16} - 800032x^{15} + 9856374x^{14} + 52362168x^{13} - 32040725x^{12} \\ & + 279370098x^{11} + 1464085056x^{10} + 1129229689x^{9} + 3299556862x^{8} \\ & + 14586202192x^{7} + 29414918270x^{6} + 45332850431x^{5} - 6437110763x^{4} \\ & - 111429920358x^{3} - 12449542097x^{2} + 93960798341x - 31890957224 \end{aligned}$$

Mascot, Zeng, Tian ($\#\mathbb{F} \leq 41$).

Question

Can we compute the image of a residual modular Galois representation without computing the representation?

Main ingredients:

1. Classification of possible images
2. Serre's conjecture

1. Classification of possible images

Theorem (Dickson)

Let ℓ be an odd prime and H a finite subgroup of $\mathsf{PGL}_2(\overline{\mathbb{F}}_\ell)$. Then a conjugate of H is one of the following groups:

- a finite subgroup of the upper triangular matrices;
- $\mathsf{PSL}_2(\mathbb{F}_{\ell^r})$ or $\mathsf{PGL}_2(\mathbb{F}_{\ell^r})$ for $r \in \mathbb{Z}_{>0}$;
- a dihedral group D_{2n} with $n \in \mathbb{Z}_{>1}$, $(\ell, n) = 1$;
- or it is isomorphic to A_4, S_4 or A_5.

Definition

If $G := \rho_f(\mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ has order prime to ℓ we call the image **exceptional**.

The field of definition of the representation is the smallest field $\mathbb{F} \subset \overline{\mathbb{F}}_\ell$ over which ρ_f is equivalent to all its conjugate. The image of the representation ρ_f is then a subgroup of $\mathsf{GL}_2(\mathbb{F})$.

Let $\mathbb{P}\rho_f : \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathsf{PGL}_2(\mathbb{F})$ be the projective representation associated to the representation ρ_f:

$$\begin{array}{ccc} \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \xrightarrow{\rho_f} & \mathsf{GL}_2(\mathbb{F}) \\ & \searrow^{\mathbb{P}\rho_f} & \downarrow{\scriptstyle \pi} \\ & & \mathsf{PGL}_2(\mathbb{F}). \end{array}$$

The representation $\mathbb{P}\rho_f$ can be defined on a different field than the field of definition of the representation. This field is called the **Dickson's field** for the representation.

2 Serre's conjecture

Theorem (Khare, Wintenberger, Dieulefait, Kisin), Serre's Conjecture

Let ℓ be a prime number and let $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be an odd, absolutely irreducible, continuous representation. Then ρ is **modular** of level $N(\rho)$, weight $k(\rho)$ and character $\epsilon(\rho)$.

- $N(\rho)$ (the level) is the Artin conductor away from ℓ.
- $k(\rho)$ (the weight) is given by a recipe in terms of $\rho|_{I_\ell}$.
- $\epsilon(\rho)\colon (\mathbb{Z}/N(\rho)\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ is given by:

$$\det \rho = \epsilon(\rho)\chi_\ell^{k(\rho)-1},$$

where χ_ℓ is the cyclotomic character mod ℓ.

The algorithm

Theorem

There is a polynomial time algorithm which takes as **input***:*

- *n and k positive integers, n is given with its factorization;*
- *ℓ a prime not dividing n and such that $2 \leq k \leq \ell + 1$;*
- *a character $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$;*
- *a morphism of ring $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$, i.e. the images of all diamond operators and of the T_p operators up to a* **bound** *$B(n, k)$,*

and gives as **output** *the image of the associated Galois representation ρ_f, up to conjugacy as subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ without computing ρ_f.*

In almost all cases, the bound $B(n,k)$ is the Sturm Bound for $\Gamma_0(n)$ and weight k:

$$B(n,k) = \frac{k}{12} \cdot n \cdot \prod_{p|n \text{ prime}} \left(1 + \frac{1}{p}\right) \ll \frac{k}{12} \cdot n \log\log n$$

In the cases when this bound is not enough, then the Sturm Bound for $\Gamma_0(nq^2)$ and weight k, where q is the smallest odd prime not dividing n, is the required bound.

For an input as in the previous slide we run into the following problem:

Problems

- ρ_f can arise from **lower level** or **weight**: there exists $g \in S(m,j)_{\overline{\mathbb{F}}_\ell}$ with $m \leq n$ or $j \leq k$ such that

$$\boxed{\rho_g \cong \rho_f}$$

- ρ_f can arise as **twist** of a representation of lower level or weight: there exist a character χ and $g \in S(m,j)_{\overline{\mathbb{F}}_\ell}$ with $m \leq n$ or $j \leq k$ such that

$$\boxed{\rho_g \otimes \chi \cong \rho_f}$$

Algorithm

- Iteration "down to top", i.e. considering all divisors of n: creation of a database
- Determine minimality with respect to level and with respect to weight.
- Determine minimality up to twisting.

Algorithm

- **Step 1** Iteration "down to top"
- **Step 2** Determine minimality with respect to level and weight.
- **Step 3** Determine whether reducible or irreducible.
- **Step 4** Determine minimality up to twisting.
- **Step 5** Compute the projective image
- **Step 6** Compute the image

Remarks

- Reducibility is checked by comparing with systems of eigenvalues coming from specific Eisenstein series.
- Compute the field of definition of the representation: this can be done using coefficients up to a finite bound.
- Compute the Dickson's field: this is obtained twisting.
- The projective image is determined by excluding cases. Each case is related to an explicit equality of mod ℓ modular forms or construction.

Setting $(*)$

- n and k positive integers;
- ℓ a prime not dividing n and such that $2 \leq k \leq \ell + 1$;
- $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ a character;
- $f : \mathbb{T}_\epsilon(n, k) \to \overline{\mathbb{F}}_\ell$ a morphism of rings;
- $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ the unique, up to isomorphism, continuous semi-simple representation attached to f;
- $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $\det(\rho_f) = \overline{\epsilon}\chi_\ell^{k-1}$.

Let p be a prime dividing $n\ell$. Let us denote by

- $G_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \subset G_{\mathbb{Q}}$ the decomposition subgroup at p;
- I_p the inertia subgroup;
- $G_{i,p}$, with $i \in \mathbb{Z}_{>0}$, the higher ramification subgroups;
- $\mathrm{N}_p(\rho)$ the valuation at p of the Artin conductor of ρ, where ρ is a residual representation.

Theorem (Gross-Vignéras-Fontaine, Serre: Conjecture 3.2.6$_?$)

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$ be a continuous, odd, irreducible representation of the absolute Galois group over $\mathbb{Q}$ to a 2-dimensional $\overline{\mathbb{F}}_\ell$-vector space V.
Let $f \in S(\mathrm{N}(\rho), k(\rho))_{\overline{\mathbb{F}}_\ell}$ be an eigenform such that $\rho_f \cong \rho$.
Let p be a prime divisor of ℓn.

(1) *If $f(T_p) \neq 0$, then there exists a stable line $D \subset V$ for the action of G_p, such that I_p acts trivially on V/D. Moreover, $f(T_p)$ is equal to the eigenvalue of Frob_p which acts on V/D.*

(2) *If $f(T_p) = 0$, then there exists no stable line $D \subset V$ as in (1).*

(1) $\Rightarrow \rho_f|_{G_p}$ is reducible;

(2) $\Rightarrow \rho_f|_{G_p}$ is irreducible.

From now on we will assume setting $(*)$.

Proposition

Let us suppose that ρ_f is irreducible and it does not arise from lower level. Let p be a prime dividing n such that $f(T_p) \neq 0$.
Then $\rho_f|_{G_p}$ is decomposable if and only if $\rho_f|_{I_p}$ is decomposable.

This proposition is proved using representation theory.

Can we deduce a computational criterion from this?

Proposition

Assume that ρ_f is irreducible and it does not arise from lower level. Let p be a prime dividing n, such that $f(T_p) \neq 0$. Then:

(A) *$\rho_f|_{I_p}$ is decomposable if and only if $\mathrm{N}_p(\rho_f) = \mathrm{N}_p(\overline{\epsilon})$;*

(B) *$\rho_f|_{I_p}$ is indecomposable if and only if $\mathrm{N}_p(\rho_f) = 1 + \mathrm{N}_p(\overline{\epsilon})$.*

Sketch of the proof

The valuation of $\mathrm{N}(\rho_f)$ at p is given by:

$$\mathrm{N}_p(\rho_f) = \sum_{i \geq 0} \frac{1}{[G_{0,p} : G_{i,p}]} \dim(V/V^{G_{i,p}}) = \dim(V/V^{I_p}) + b(V),$$

where V is the two-dimensional $\overline{\mathbb{F}}_\ell$-vector space underlying the representation, $V^{G_{i,p}}$ is the subspace of invariants under $G_{i,p}$, and $b(V)$ is the wild part of the conductor.
Since $f(T_p) \neq 0$, the representation restricted to the decomposition group at p is reducible. Hence, after conjugation,

$$\rho_f|_{G_p} \cong \begin{pmatrix} \epsilon_1 \chi_\ell^{k-1} & * \\ 0 & \epsilon_2 \end{pmatrix}, \quad \rho_f|_{I_p} \cong \begin{pmatrix} \epsilon_1|_{I_p} & * \\ 0 & 1 \end{pmatrix}$$

where ϵ_1 and ϵ_2 are characters of G_p with ϵ_2 unramified, χ_ℓ is the mod ℓ cyclotomic character and $*$ belongs to $\overline{\mathbb{F}}_\ell$.

Sketch of the proof

$$\rho_f|_{I_p} \cong \begin{pmatrix} \epsilon_1|_{I_p} & * \\ 0 & 1 \end{pmatrix}.$$

If $\rho_f|_{I_p}$ is indecomposable ($* \neq 0$) then V^{I_p} is either $\{0\}$ if ϵ_1 is ramified, or $\overline{\mathbb{F}}_\ell \cdot \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ if ϵ_1 is unramified. The wild part of the conductor is equal to the wild part of the conductor of ϵ_1. Hence, we have that

$$\mathrm{N}_p(\rho_f) = \begin{cases} 1 = 1 + \mathrm{N}_p(\epsilon_1) & \text{if } \epsilon_1 \text{ is unramified,} \\ 2 + b(\epsilon_1) = 1 + \mathrm{N}_p(\epsilon_1) & \text{if } \epsilon_1 \text{ is ramified.} \end{cases}$$

Since $\det(\rho_f) = \overline{\epsilon}\chi_\ell^{k-1}$, then $\det(\rho_f)|_{I_p} = \overline{\epsilon}|_{I_p}$, so $\epsilon_1|_{I_p} = \overline{\epsilon}|_{I_p}$. Therefore, we have that if $\rho_f|_{I_p}$ is indecomposable then $\mathrm{N}_p(\rho_f) = 1 + \mathrm{N}_p(\overline{\epsilon})$.

The other case is analogous.

Assume setting $(*)$ and that ρ_f is irreducible and it does not arise from lower level or weight.

Then ρ_f can still arise as twist of a representation of lower level or weight, i.e. there exist $g \in S(m,j)_{\overline{\mathbb{F}}_\ell}$ with $m \leq n$ or $j \leq k$ and a character χ such that $\rho_g \otimes \chi \cong \rho_f$.

Question

Can we compute twists?

For this talk, we limit ourselves to study twists of modular Galois representations by Dirichlet characters with prime power conductor coprime with the characteristic.

Question

What is the **conductor** of the twist?

Shimura gave an upper bound:

$$\boxed{\mathrm{lcm}(\mathrm{cond}(\chi)^2, n)}$$

where n is the level of the form and χ is the Dirichlet character used for twisting.

Proposition

Let p be a prime **not** *dividing $n\ell$. Let $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$, for $i > 0$, be a non-trivial character. Then*

$$\mathrm{N}_p(\rho_f \otimes \chi) = 2\mathrm{N}_p(\chi).$$

Proposition

Assume that ρ_f is irreducible and it does not arise from lower level. Let p be a prime dividing n and suppose that $\boxed{f(T_p) \neq 0}$.

Let $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$, for $i > 0$, be a non-trivial character. Then

$$\mathrm{N}_p(\rho_f \otimes \chi) = \mathrm{N}_p(\chi\bar{\epsilon}) + \mathrm{N}_p(\chi).$$

It is also possible to know what is the **system of eigenvalues** associated to the twist:

Proposition

Suppose that ρ_f is irreducible and that $\mathrm{N}(\rho_f) = n$. Let p be a prime dividing n and suppose that $f(T_p) \neq 0$. Let χ from $(\mathbb{Z}/p^i\mathbb{Z})^*$ to $\overline{\mathbb{F}}_\ell^*$, with $i > 0$, be a non-trivial character. Then

(A) *if $\rho_f|_{I_p}$ is decomposable then the representation $\rho_f \otimes \chi$, restricted to G_p, admits a stable line with unramified quotient if and only if $\mathrm{N}_p(\rho_f \otimes \chi) = \mathrm{N}_p(\rho_f)$;*

(B) *if $\rho_f|_{I_p}$ is indecomposable then the representation $\rho_f \otimes \chi$, restricted to G_p, does not admit any stable line with unramified quotient.*

(A) $\Rightarrow (\rho_f \otimes \chi)(\mathrm{Frob}_p) \neq 0$;

(B) $\Rightarrow (\rho_f \otimes \chi)(\mathrm{Frob}_p) = 0$;

Analogous result holds when $f(T_p) = 0$, where $p \mid \mathrm{N}(\rho_f)$:

Proposition

Suppose that ρ_f is irreducible and that $\mathrm{N}(\rho_f) = n$. Let p be a prime dividing n and suppose that $\boxed{f(T_p) = 0}$. Then:

(A) *if $\rho_f|_{G_p}$ is reducible then there exists a mod ℓ modular form g of weight k and level at most np and a non-trivial character $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ with $i > 0$ such that $g(T_p) \neq 0$ and $\rho_g \cong \rho_f \otimes \chi$;*

(B) *if $\rho_f|_{G_p}$ is irreducible then for any non-trivial character $\chi : (\mathbb{Z}/p^i\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ with $i > 0$ the representation $\rho_f \otimes \chi$ restricted to G_p does not admit any stable line with unramified quotient.*

Example: let $n = 135 = 3^3 5$. Let ϵ be the Dirichlet character modulo 135 of conductor 5 mapping $56 \to 1$, $82 \to \zeta_{36}^{9}$.

$S(135, 3, \epsilon)_{\mathbb{C}}^{\mathrm{new}}$ two Galois orbits, the two Hecke eigenvalue fields are:
$\mathbb{Q}\left(x^{16} + 217x^{12} + 9264x^8 + 59497x^4 + 28561\right)$ and
$\mathbb{Q}\left(x^{16} + 286x^{12} + 16269x^8 + 85684x^4 + 62500\right)$.

We want to compute the image of the mod 7 representations attached to the reduction of the forms in the first Galois orbit.

Applying the reduction map for all prime ideals above 7, we obtain the following eigenvalue systems defined over $\mathbb{F}_7[x]/[x^2 + 6x + 4] \cong \mathbb{F}_7[\alpha]$:

p	$f_1(T_p)$	$f_2(T_p)$	$f_3(T_p)$
2	α	6α	$\alpha+6$
3	0	0	0
5	$5\alpha+4$	$2\alpha+3$	$5\alpha+5$
7	0	0	0
11	$\alpha+3$	$6\alpha+4$	$\alpha+3$
13	6α	6α	$\alpha+6$
17	6α	α	$6\alpha+1$
19	$6\alpha+4$	$6\alpha+4$	$\alpha+3$
23	$3\alpha+4$	$4\alpha+3$	3α

f_1, f_2 and f_3 are mod 7 modular forms of level 135 and weight 3.

It is easy to verify that the corresponding representations are of minimal level and weight.

Let us focus on f_1.

p	$f_1(T_p)$	$f_2(T_p)$	$f_3(T_p)$
2	α	6α	$\alpha+6$
3	0	0	0
5	$5\alpha+4$	$2\alpha+3$	$5\alpha+5$
7	0	0	0
11	$\alpha+3$	$6\alpha+4$	$\alpha+3$
13	6α	6α	$\alpha+6$
17	6α	α	$6\alpha+1$
19	$6\alpha+4$	$6\alpha+4$	$\alpha+3$
23	$3\alpha+4$	$4\alpha+3$	3α

Since 5 divides the level and $f_1(T_5) \neq 0$:

$$\rho_{f_1}|_{G_5} \cong \begin{pmatrix} \epsilon_1\chi_7^2 & * \\ 0 & \epsilon_2 \end{pmatrix} \cong \begin{pmatrix} \epsilon_2^{-1}\epsilon_{f_1}\chi_7^2 & 0 \\ 0 & \epsilon_2 \end{pmatrix}$$

The character ϵ_{f_1} attached to f_1 has conductor 5, hence the representation is reducible and decomposable, so $* = 0$.
Moreover $\epsilon_2(5) = f_1(T_5) = 5\alpha + 4$.

If we twist by $\epsilon_{f_1}^{-1}$ then we have:

$$(\rho_{f_1} \otimes \epsilon_{f_1}^{-1})|_{G_5} \cong \begin{pmatrix} \epsilon_2^{-1}\chi_7^2 & 0 \\ 0 & \epsilon_2\epsilon_{f_1}^{-1} \end{pmatrix}$$

The conductor of the twist is 135, the eigenvalues at primes $p \neq 5$ are given by $f(T_p)\epsilon_{f_1}^{-1}(p)$ while the eigenvalue at 5 is

$$(\epsilon_2^{-1}\chi_7^2)(5) = 4\epsilon_2^{-1}(5) = 5\alpha + 5.$$

p	$f_1(T_p)$	$f_2(T_p)$	$f_3(T_p)$	$\rho_{f_1} \otimes \epsilon_{f_1}^{-1}$
2	α	6α	$\alpha+6$	$\alpha+6$
3	0	0	0	0
5	$5\alpha+4$	$2\alpha+3$	$5\alpha+5$	$5\alpha+5$
7	0	0	0	0
11	$\alpha+3$	$6\alpha+4$	$\alpha+3$	$\alpha+3$
13	6α	6α	$\alpha+6$	$\alpha+6$
17	6α	α	$6\alpha+1$	$6\alpha+1$
19	$6\alpha+4$	$6\alpha+4$	$\alpha+3$	$\alpha+3$
23	$3\alpha+4$	$4\alpha+3$	3α	3α
29	2	5	5	5
31	4	4	4	4
37	$\alpha+6$	$\alpha+6$	6α	6α
41	$5\alpha+1$	$2\alpha+6$	$5\alpha+1$	$5\alpha+1$

$$\rho_{f_1} \otimes \epsilon_{f_1}^{-1} \cong \rho_{f_3}$$

The level is also divisible by 3. But $f_1(T_3) = 0$.

The local representation at 3 is irreducible: to prove this claim we have to check all lover levels and possible twist.
In this case it is easy, since the newforms space is empty in most cases.
The argument is similar for all levels, let us what happens for level 15.

p	$f_1(T_p)$	$g_1(T_p)$	$g_2(T_p)$	$g_3(T_p)$	$g_4(T_p)$
2	α	$6\alpha+6$	$\alpha+5$	$4\alpha+1$	$3\alpha+5$
3	0	6α	$\alpha+6$	α	$6\alpha+1$
5	$5\alpha+4$	$3\alpha+5$	$4\alpha+1$	$2\alpha+1$	$5\alpha+3$
7	0	$4\alpha+5$	$3\alpha+2$	2	2
11	$\alpha+3$	$6\alpha+1$	α	α	$6\alpha+1$
13	6α	$4\alpha+5$	$3\alpha+2$	5	5

It is possible to show that

$$\mathbb{P}\rho_{f_1}(G_{\mathbb{Q}}) \cong \mathsf{PSL}_2(\mathbb{F}_7) \subset \mathsf{PGL}_2(\mathbb{F}_{7^2}),$$

and that the image of the Galois representation up to conjugation is

$$\rho_{f_1}(G_{\mathbb{Q}}) \cong < \alpha > \mathsf{SL}_2(\mathbb{F}_7) \subset \mathsf{GL}_2(\mathbb{F}_{7^2})$$

An application of the study of twists is the computation of the field of definition of the representation and of the projective representation associated.

Field of definition of the representation:

Proposition

Suppose that ρ_f is irreducible and does not arise from lower level or weight. Then the field of definition of ρ_f is the smallest extension of $\mathbb{F}_\ell$ containing the elements of the set

$$S := \{f(T_p) |\, p \text{ prime, } p \neq \ell \text{ and } p \leq B(n,k)\} \cup \{f(\langle d \rangle) |\, d \in (\mathbb{Z}/n\mathbb{Z})^*\},$$

where $B(n,k)$ is the Sturm bound for cusp forms for $\Gamma_0(n)$.

Field of definition of the projective representation $\mathbb{P}\rho_f$

Proposition

Let us suppose that ρ_f is irreducible, it does not arise from lower level or weight and it is realized over $\mathbb{F}$. Then the field of definition of $\mathbb{P}\rho_f$ is the subfield of $\mathbb{F}$ fixed by

$$A := \left\{\sigma \in \mathsf{Aut}(\mathbb{F}) |\ \exists \tau : \mathsf{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}^* : \rho_f^\sigma \cong \rho_f \otimes \tau\right\}.$$

Proposition

Assume that ρ_f is irreducible, does not arise from lower level or weight and is realized over $\mathbb{F}$. Then the field of definition of $\mathbb{P}\rho_f$ is the smallest extension of $\mathbb{F}_\ell$ containing

$$(f(T_p))^2/f(\langle p\rangle)p^{k-1}$$

for all p prime, $p \nmid n\ell$.

This proposition is not effective: there is no bound for the number of traces needed. Anyway, combining it with the previous, there is an algorithm to compute the Dickson's field.

Proposition

Let $p \geq 5$ be a prime and $r \geq 1$ be an integer. Then there are no solutions to

$$17^r x^p + 2y^p = z^2$$

for non-zero coprime integers x, y, z.

Proof

If $xy = \pm 1$, then there is no solution (reduce modulo 8).
If $xy \neq \pm 1$, then, without loss of generality, we can assume that $17^r x$, $2y$ and z are coprime, $1 \leq r < p$, and xy is odd. The solutions are then related to the Frey curve

$$E : Y^2 + XY = X^3 + 2zX^2 + 2y^p X$$

which has minimal discriminant $2^8 17^r (xy^2)^p$ and conductor $2^7 \mathrm{Rad}(17xy)$.

Proof.

It is possible to show that:

- E does not have complex multiplication
- E arises mod ℓ from some newform $f \in S(2^7 17, 2)$ for primes ℓ dividing a constant given by an explicit recipe by Mazur. For example $\ell = 3$ works.

There are 16 Galois orbits of newforms of level $2^7 17$ weight 2 which all are irrational.

The mod 3 representation cannot arise from a lower level: this would contradict Ribet's Level-Lowering Theorem. It is irreducible because the Frey curve does not admit 3 isogenies.

The field of definitions of the mod 3 Galois representations associated to each of these newforms is larger than $\mathbb{F}_3$: for all the newforms the reduction of $f(T_5) \notin \mathbb{F}_3$. Contradiction. $\square$

Work on progress, joint with Vandita Patel (University of Warwick).

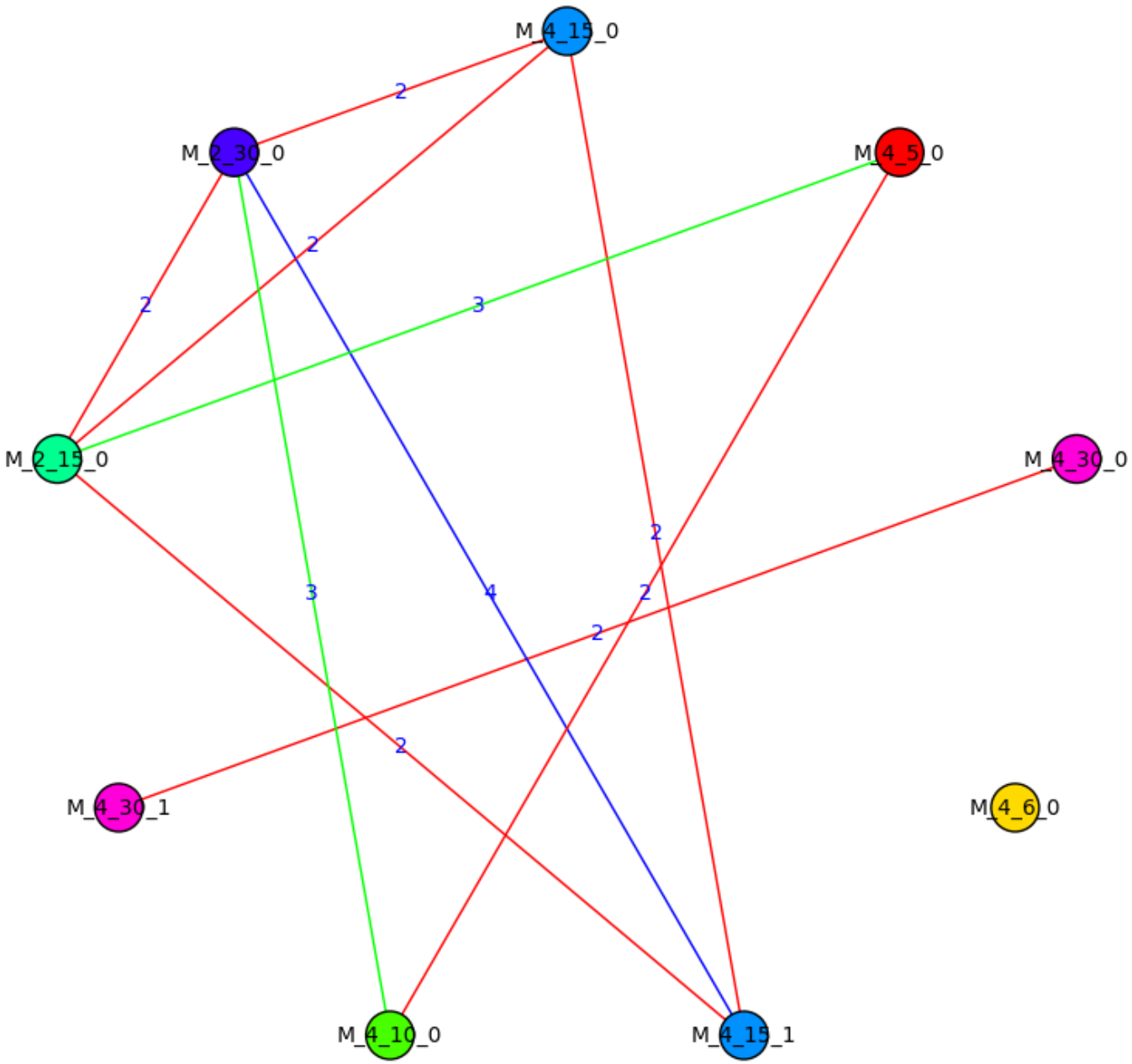
Idea: build graphs of congruences between modular forms and enrich these graphs using datas coming form residual representations.

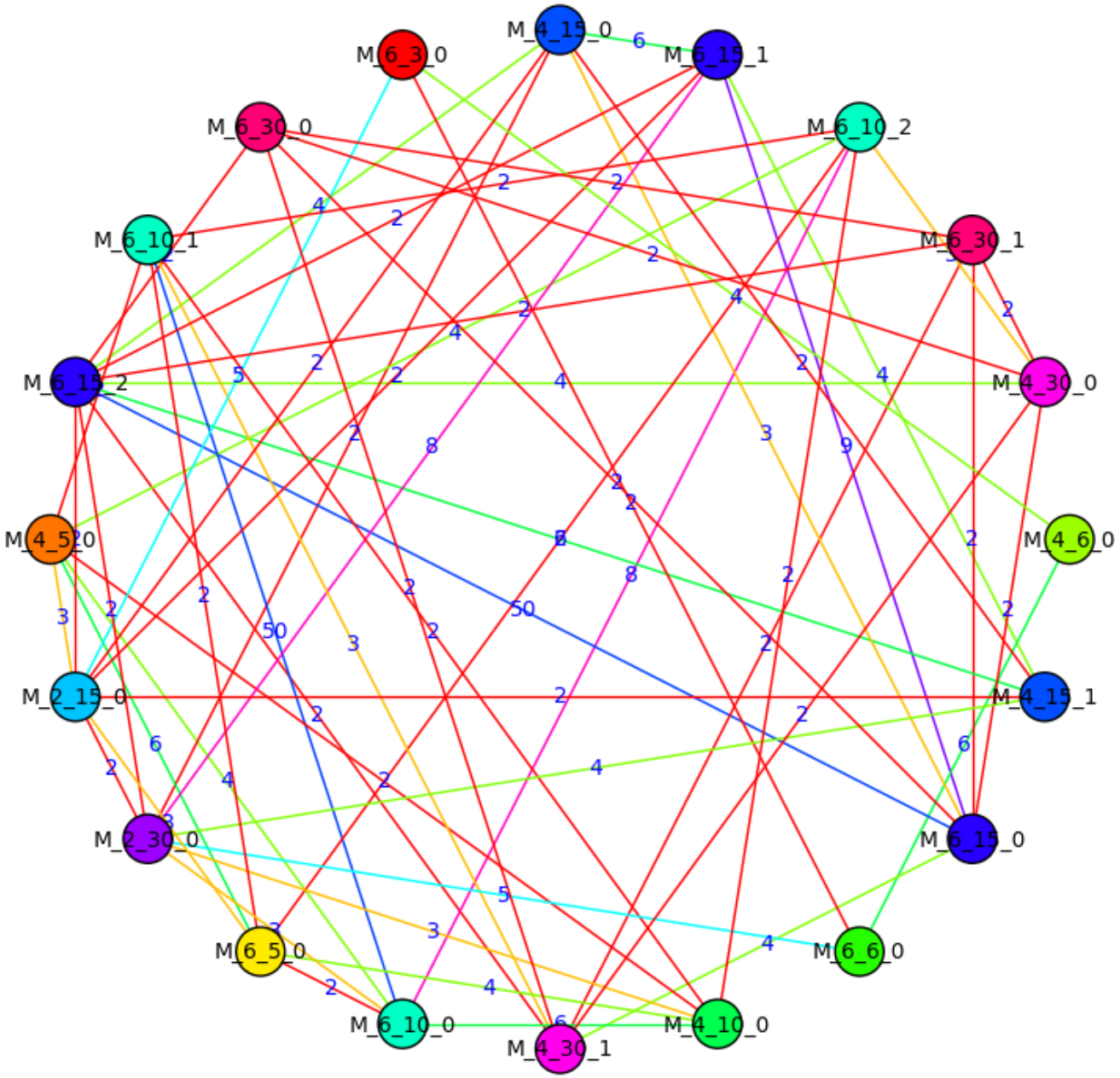
- Vertices: newforms of levels and weights in a given set;
- Edges: an eadge between two verices is drawn if a relation $\mathcal{R}$ holds.

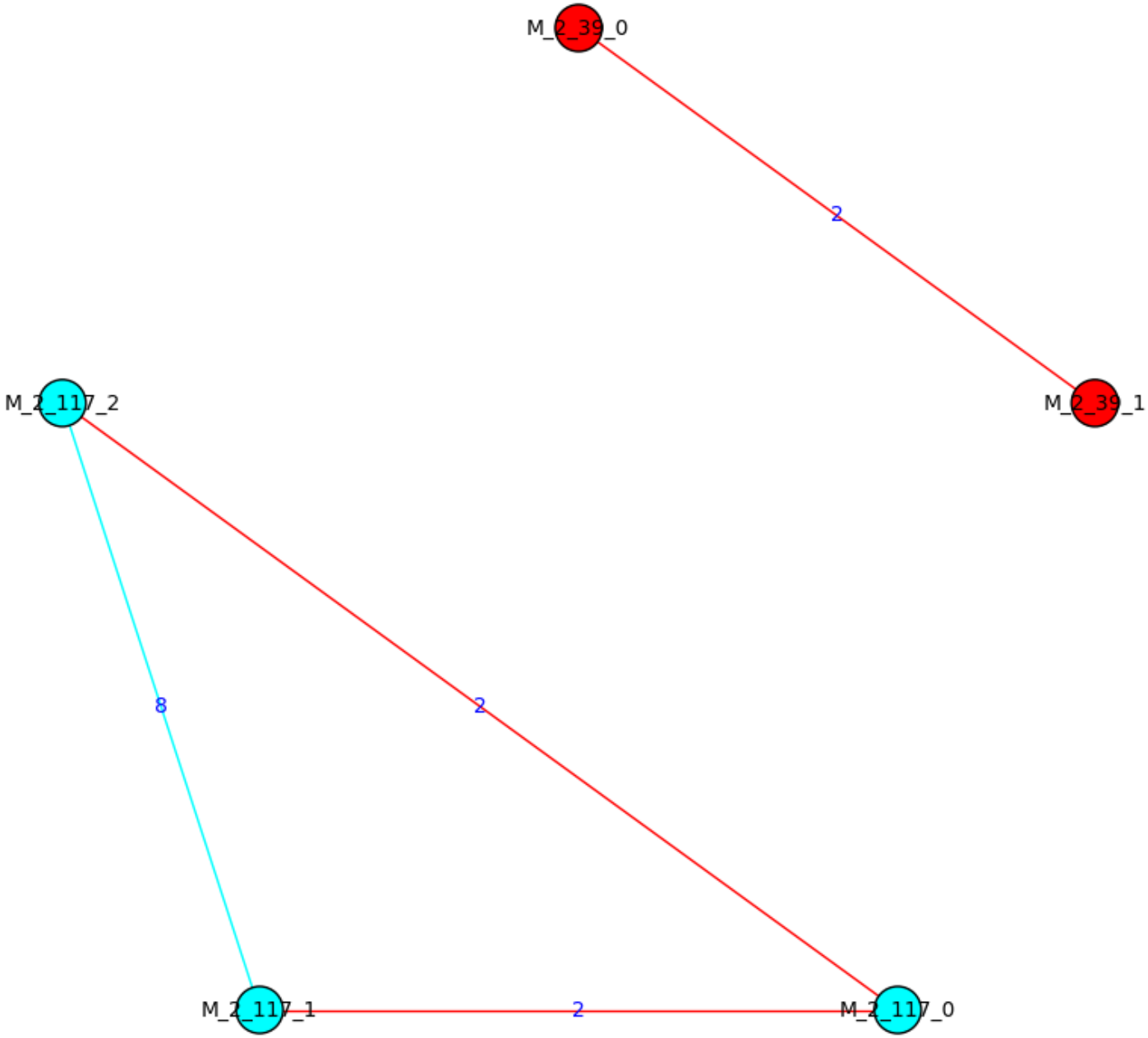
What kind of relations we are going to consider?

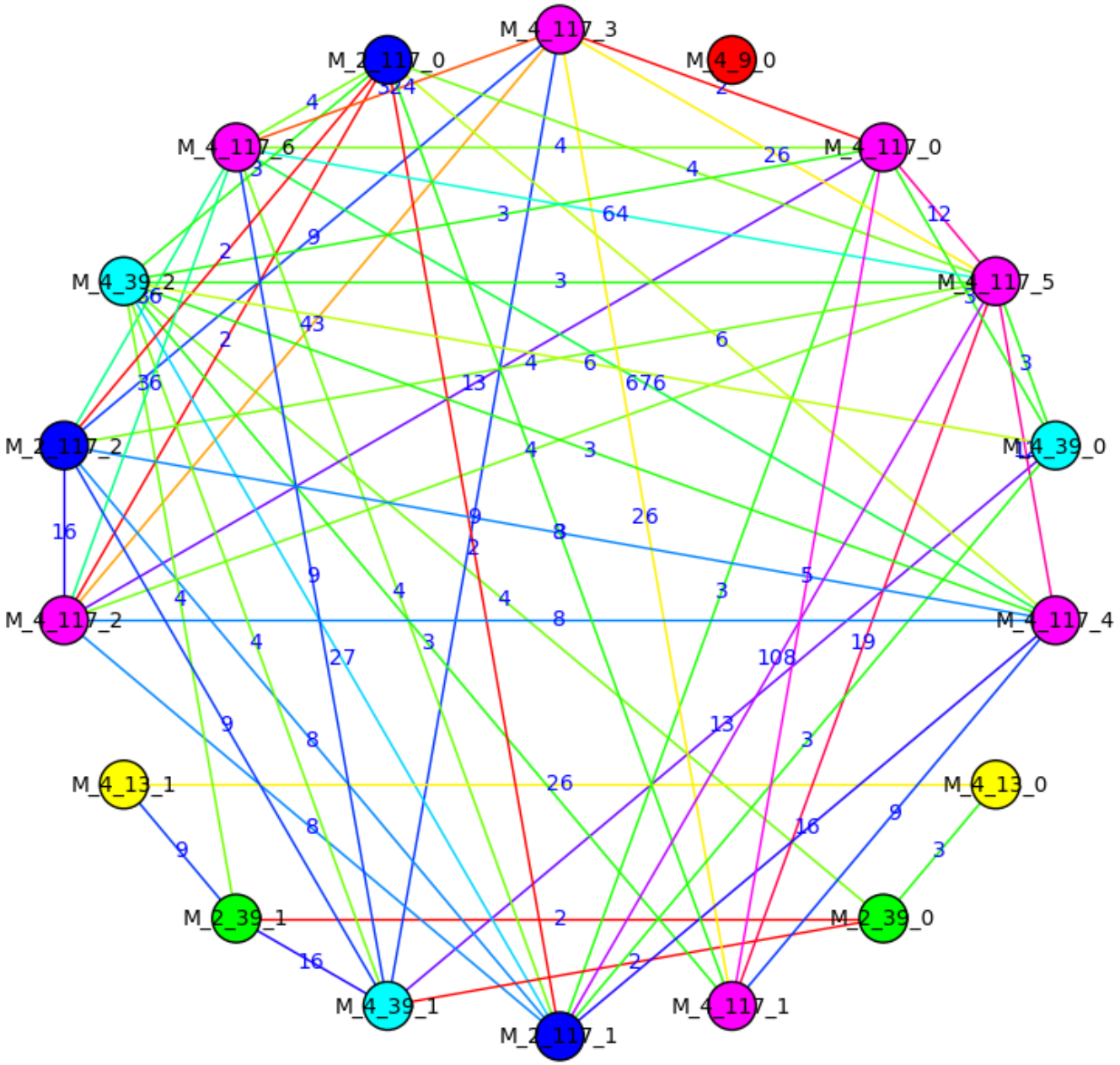
- $\mathcal{R}_1$: congruence modulo some prime ℓ;
- $\mathcal{R}_2$: isomorphic mod ℓ Galois representations for some prime ℓ;
- $\mathcal{R}_3$: isomorphic mod ℓ projective Galois representations for some prime ℓ.

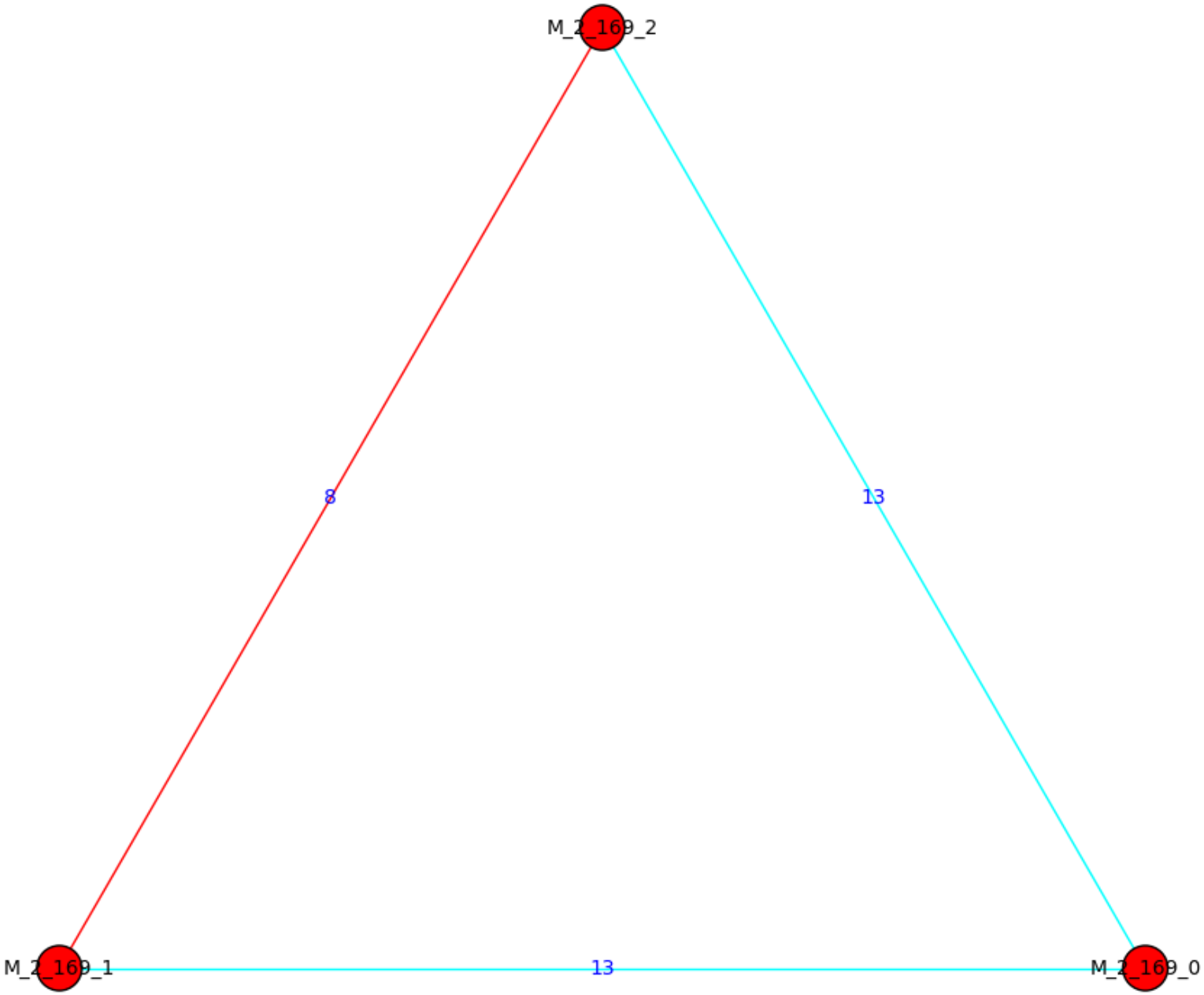
until now we implemented an algorithm which draws graphs for $\mathcal{R}_1$.

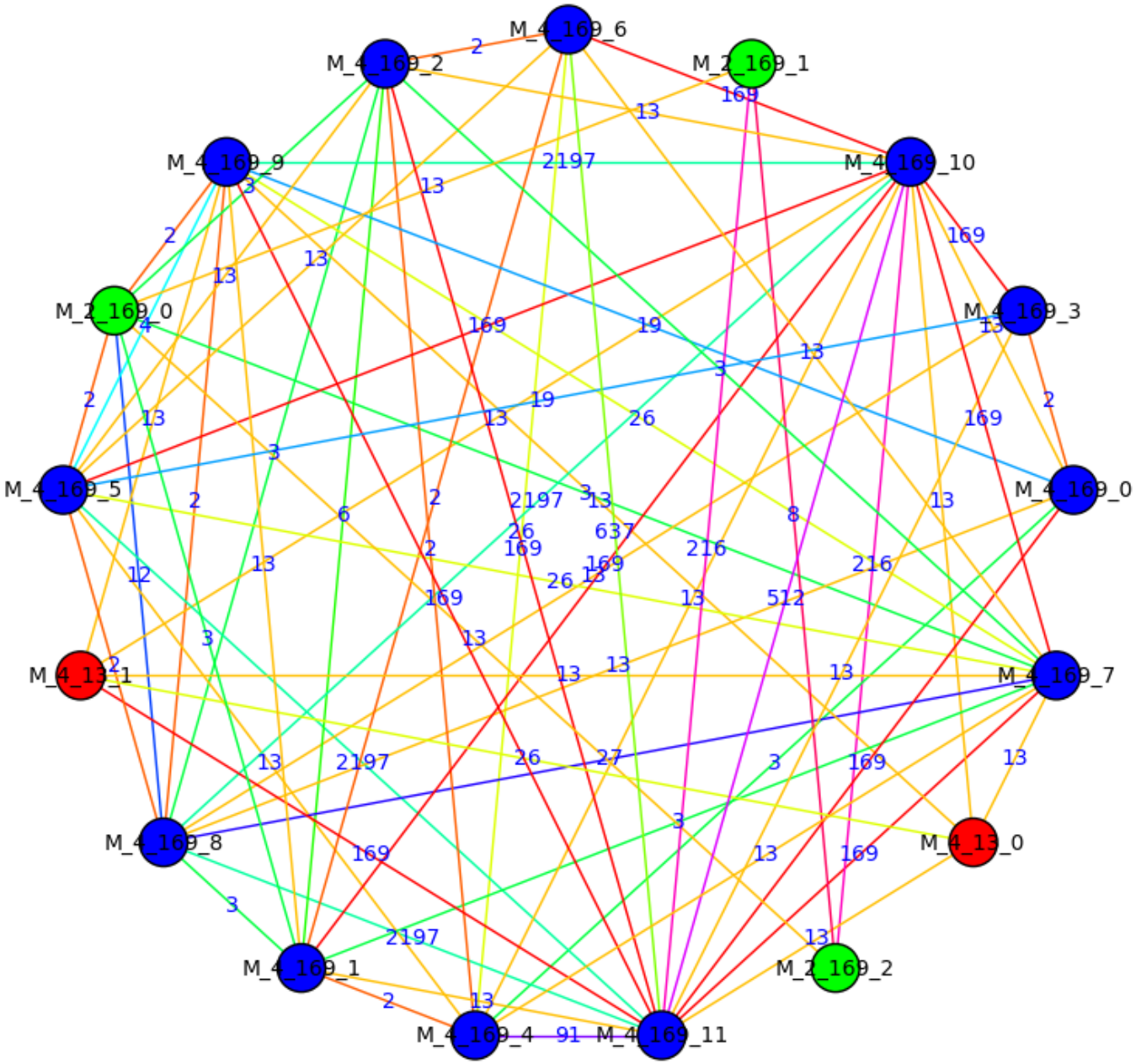

M_4_15_0
M_2_30_0
M_4_5_0
M_2_15_0
M_4_30_0
M_4_30_1
M_4_6_0
M_4_10_0
M_4_15_1
2
2
2
3
2
3
4
2
2
2


M_4_15_0
M_6_3_0
M_6_15_1
M_6_30_0
M_6_10_2
M_6_10_1
M_6_30_1
M_6_15_2
M_4_30_0
M_4_5_0
M_4_6_0
M_2_15_0
M_4_15_1
M_2_30_0
M_6_15_0
M_6_5_0
M_6_6_0
M_6_10_0
M_4_10_0
M_4_30_1


M_2_39_0
2
M_2_39_1
M_2_117_2
8
2
M_2_117_1
2
M_2_117_0


M_4_117_3
M_2_117_0
M_4_9_0
M_4_117_6
M_4_117_0
M_4_39_2
M_4_117_5
M_2_117_2
M_4_39_0
M_4_117_2
M_4_117_4
M_4_13_1
M_4_13_0
M_2_39_1
M_2_39_0
M_4_39_1
M_4_117_1
M_2_117_1


M_2_169_2
8
13
M_2_169_1
13
M_2_169_0


M_4_169_6
M_4_169_2
M_2_169_1
M_4_169_9
M_4_169_10
M_2_169_0
M_4_169_3
M_4_169_5
M_4_169_0
M_4_13_1
M_4_169_7
M_4_169_8
M_4_13_0
M_4_169_1
M_2_169_2
M_4_169_4
M_4_169_11

Residual modular Galois representations: images and applications

Samuele Anni

University of Warwick

London Number Theory Seminar
King's College London, 20th May 2015

Thanks!